PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-312402
(43)Date of publication of application : 09.11.2001

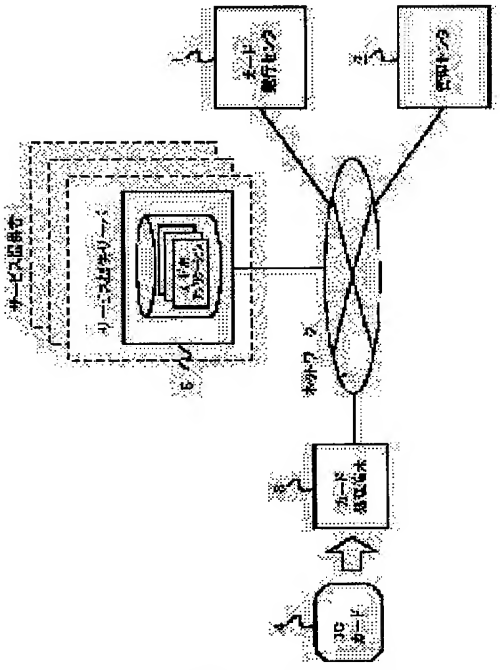
(51)Int.Cl. G06F 9/06
G06F 9/445
G06K 17/00
G06K 19/07
G06K 19/00

(21)Application number : 2000-129056
(22)Date of filing : 28.04.2000

(71)Applicant : NTT DATA CORP
(72)Inventor : YAMAZAKI KENJI
SAKAI TAKAAKI
AMAMIYA SHUNICHI
TAMAI JUN
TOMINAGA HIROSHI
TAKAGI SOICHIRO

(54) CARD SYSTEM, IC CARD, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a card system, etc., which can safely supply an application.
SOLUTION: An IC card 4 stores a permission table where the hash value of an application allowed by a card issue center 1 to be supplied is set. The IC card 4 obtains the hash value of an application supplied from a service providing server 5, decides whether the hash value matches the hash value registered in the permission table, and stores the application in a prescribed area of the IC card 4 when they match each other, but performs prescribed error processing when not.



LEGAL STATUS

[Date of request for examination] 04.04.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－312402
（P2001－312402A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｇ	５Ｂ０３５
	9/445		Ｇ０６Ｋ　17/00	Ｂ	５Ｂ０５８
Ｇ０６Ｋ	17/00			Ｄ	５Ｂ０７６
			Ｇ０６Ｆ　9/06	４２０Ｊ	
	19/07		Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2000－129056(P2000－129056)

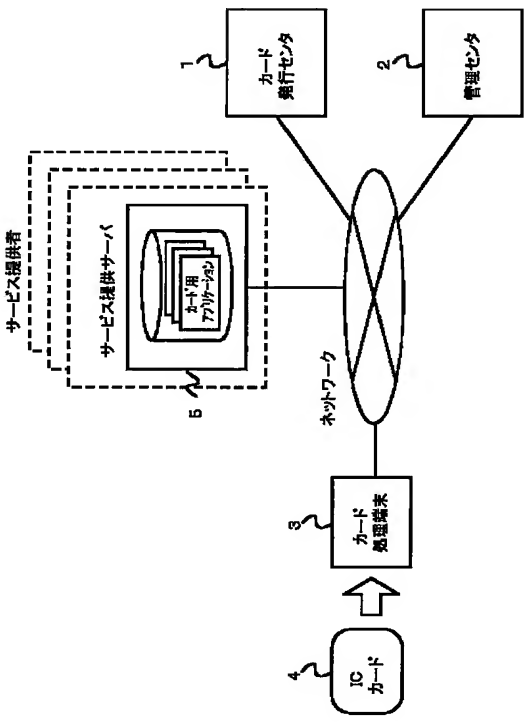
(22)出願日　平成12年４月28日(2000.4.28)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　山崎　研史
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　酒井　敬明
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

最終頁に続く

(54)【発明の名称】　カードシステム、ＩＣカード及び記録媒体

(57)【要約】
【課題】　アプリケーションの供給を安全に行うことができるカードシステム等を提供する。
【解決手段】　ＩＣカード４は、カード発行センタ１により供給が許可されたアプリケーションのハッシュ値が設定されている許可テーブルを記憶する。ＩＣカード４は、サービス提供サーバ５から供給されたアプリケーションについてハッシュ値を求め、許可テーブルに登録されているハッシュ値と合致するか否かを判別し、合致する場合、そのアプリケーションをＩＣカード４の所定領域に記憶し、合致しない場合、所定のエラー処理を行う。



【特許請求の範囲】

【請求項１】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、

前記ＩＣカードは、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項２】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーション基づいて導出されるチェック情報がそれぞれ設定され、

前記ＩＣカードは、

前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該当するアプリケーションのチェック情報と照合し、

前記チェック情報が合致する場合には、前記供給されたアプリケーションを当該ＩＣカードの所定領域に記憶し、

前記チェック情報が合致しない場合には、所定のエラー処理を行う、

ことを特徴とする請求項１に記載のカードシステム。

【請求項３】前記チェック情報はハッシュ値を含む、

ことを特徴とする請求項２に記載のカードシステム。

【請求項４】前記許可テーブルには、管理機関による署名が付与されている、

ことを特徴とする請求項１又は２に記載のカードシステム。

【請求項５】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、

前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、

前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、

前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、

前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、

ことを特徴とするＩＣカード。

【請求項６】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーション

を記憶するカードシステムであって、

前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ＩＣカードに供給し、

前記ＩＣカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、

ことを特徴とするカードシステム。

【請求項７】前記供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるＩＣカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給し、

前記ＩＣカードは、当該ＩＣカードの鍵を用いて前記認証情報の正当性をチェックする、

ことを特徴とする請求項６に記載のカードシステム。

【請求項８】供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給し、

前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証情報として前記供給センタに供給し、

前記ＩＣカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックする、

ことを特徴とする請求項６に記載のカードシステム。

【請求項９】前記ＩＣカードは、当該ＩＣカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給し、

前記供給センタは、前記ＩＣカードからの削除証明書を前記カード発行センタに送信する、

ことを特徴とする請求項６乃至８のいずれか１項に記載のカードシステム。

【請求項１０】カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、

前記ＩＣカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、

3

前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、
ことを特徴とするＩＣカード。
【請求項１１】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
該コンピュータを、
前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、
前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、
前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該ＩＣカードの所定領域に記憶する手段、
前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１２】コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
該コンピュータを、
前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、
前記認証情報の正当性をチェックする手段、
前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶する手段、
前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、
として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、カード発行センタにより発行されたＩＣカードに、アプリケーションの供給を行う供給センタにより供給されるアプリケーションを記憶するカードシステム等に関する。
【０００２】
【従来の技術】例えばカード発行者が各利用者に対して発行したＩＣカードに、アプリケーションの供給者（サービス提供者）がカード用アプリケーションを供給して、ＩＣカードの多目的利用を図るカードシステムが知られている。このようなシステムでは、例えば、利用者

4

は所望のアプリケーションを自己のＩＣカードにダウンロードし、ＩＣカードに組み込まれたアプリケーションを実行させることにより、サービス提供者による所定のサービスを受けることができる。
【０００３】
【発明が解決しようとする課題】上記のようなカードシステムでは、例えば不正なサービス提供者によるＩＣカードへのアプリケーションの供給を防止し、安全にアプリケーションの供給が受けられる仕組みが必要とされている。
【０００４】また、システムの安全性を保持する観点からアプリケーションの供給者（サービス提供者）の認証処理を行う場合、その認証処理が複雑化・長時間化してしまうと、システムのレスポンスを低下させてしまうおそれがある。
【０００５】また、カード発行者により各ＩＣカードへのアプリケーションの供給状況が正確に把握され、例えば各サービス提供者への適正な課金管理が実現されること等が業界において望まれている。
【０００６】本発明は、上述した事情に鑑みてなされたもので、アプリケーションの供給を安全に行うことができるカードシステム等を提供することを目的とする。また、本発明は、アプリケーションの供給者の認証処理の複雑化・長時間化を防止することができるカードシステム等を提供することを他の目的とする。また、本発明は、ＩＣカードへのカード用アプリケーションの登録状況の管理が可能なシステム等を提供することを他の目的とする。
【０００７】
【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点に係るカードシステムは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記ＩＣカードは、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う。
【０００８】このような構成によれば、ＩＣカードに予めカード発行センタが許可したアプリケーションに関する許可テーブルを格納しておき、ＩＣカードにアプリケーションをダウンロードする際に、そのアプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタにアプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安

全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【０００９】前記許可テーブルには、各前記アプリケーションについて、当該アプリケーション基づいて導出されるチェック情報がそれぞれ設定されてもよく、前記ＩＣカードは、前記供給センタからのアプリケーションの供給に応答し、前記供給されたアプリケーションに基づいてチェック情報を導出し、前記許可テーブルに設定されている該当するアプリケーションのチェック情報と照合してもよく、前記チェック情報が合致する場合には、前記供給されたアプリケーションを当該ＩＣカードの所定領域に記憶してもよく、前記チェック情報が合致しない場合には、所定のエラー処理を行ってもよい。

【００１０】前記チェック情報はハッシュ値を含んでもよい。

【００１１】前記許可テーブルには、管理機関による署名が付与されていてもよい。これにより、許可テーブルを用いてアプリケーションのチェックを行うことは、カード発行センタと管理機関の両方からの許可を確認することと実質的に同意となるため、さらにシステムの安全性を高めることができる。また、第三者的な管理機関による署名を付与することで、例えばカード発行元とアプリケーション供給者（サービス提供者）の共同による不正行為等を防止することができる。

【００１２】また、本発明の第２の観点に係るＩＣカードは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステム用のＩＣカードであって、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶し、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別し、前記アプリケーションが前記許可テーブルに登録されている場合、該アプリケーションを当該ＩＣカードの所定領域に記憶し、前記アプリケーションが前記許可テーブルに登録されていない場合、所定のエラー処理を行う、ことを特徴とする。

【００１３】また、本発明の第３の観点に係るカードシステムは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記憶するカードシステムであって、前記供給センタは、前記カード発行センタから認証情報を取得し、取得した前記認証情報とアプリケーションを前記ＩＣカードに供給し、前記ＩＣカードは、前記供給センタからの前記認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【００１４】このような構成によれば、ＩＣカードにアプリケーションを供給する時にはカード発行センタにより発行される認証情報が必要とされる。これにより、カード発行センタから認証情報を取得していないサービス提供サーバによるＩＣカードへのアプリケーションの登録を排除し、安全なカードシステムを提供することができる。

【００１５】前記供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードからカード識別符号を取得し、取得した前記カード識別符号とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記アプリケーション識別符号に基づくアプリケーションに関する情報を、前記カード識別符号により特定されるＩＣカードの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ＩＣカードは、当該ＩＣカードの鍵を用いて前記認証情報の正当性をチェックしてもよい。

【００１６】また、供給センタは、ＩＣカードにアプリケーションを供給するとき、アプリケーションの供給先のＩＣカードから乱数を取得し、取得した乱数とアプリケーション識別符号を前記カード発行センタに供給してもよく、前記カード発行センタは、前記乱数と前記アプリケーション識別符号に基づくアプリケーションに関する情報を当該カード発行センタの鍵で暗号化したものを前記認証情報として前記供給センタに供給してもよく、前記ＩＣカードは、乱数を生成して前記供給センタに供給し、前記供給センタから供給された前記認証情報の正当性を前記カード発行センタの鍵を用いてチェックしてもよい。

【００１７】前記ＩＣカードは、当該ＩＣカードに記憶されているアプリケーションの削除に伴い、削除対象のアプリケーションに関する削除証明書を作成し、前記削除対象のアプリケーションの供給元の供給センタに供給してもよく、前記供給センタは、前記ＩＣカードからの削除証明書を前記カード発行センタに送信してもよい。

【００１８】これにより、アプリケーションがＩＣカードに供給される度に供給センタがカード発行センタから認証情報を取得するため、カード発行センタは、各ＩＣカードへアプリケーションが供給されたことを確実に把握することができる。また、ＩＣカードがアプリケーションの削除についての証明書を供給センタに対して発行し、供給センタがその証明書をカード発行センタに提出することにより、カード発行センタは、各ＩＣカードからアプリケーションが削除されたことを確実に把握することができる。また、カード発行センタは、各ＩＣカードについて、アプリケーションの登録及び削除を確実に把握できるため、供給センタに対して適正な課金管理を行うことができる。

【００１９】また、本発明の第４の観点に係るＩＣカードは、カード発行センタにより発行されたＩＣカードに、供給センタにより供給されるアプリケーションを記

憶するカードシステム用のＩＣカードであって、前記ＩＣカードは、前記供給センタが前記カード発行センタから取得した認証情報を受け取って、該認証情報の正当性をチェックし、チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶し、チェック結果がエラーを示す場合、所定のエラー処理を行う、ことを特徴とする。

【００２０】また、本発明の第５の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを、前記カード発行センタにより供給が許可されたアプリケーションに関する許可テーブルを記憶する手段、前記供給センタから供給されたアプリケーションが前記許可テーブルに登録されているか否かを判別する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていると判別された場合、該アプリケーションを当該ＩＣカードの所定領域に記憶する手段、前記判別手段により前記アプリケーションが前記許可テーブルに登録されていないと判別された場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【００２１】また、本発明の第６の観点に係る記録媒体は、コンピュータを、カード発行センタにより発行され、供給センタにより供給されるアプリケーションを記憶するＩＣカードとして機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、該コンピュータを前記供給センタが前記カード発行センタから取得した認証情報を受け取る手段、前記認証情報の正当性をチェックする手段、前記チェック結果が正常を示す場合、前記供給センタからのアプリケーションを当該ＩＣカードの所定領域に記憶する手段、前記チェック結果がエラーを示す場合、所定のエラー処理を行う手段、として機能させるためのプログラムを記録する。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態に係るカードシステムを図面を参照して説明する。このカードシステムは、カード発行者が利用者に対して発行したＩＣカードに、アプリケーションの供給者（サービス提供者）により供給される種々のカード用アプリケーションをダウンロードして組み込むためのものである。

【００２３】（第１の実施形態）本発明の第１の実施形態に係るカードシステムのシステム構成図を図１に示す。図示されるように、このカードシステムは、カード発行センタ１と、管理センタ２と、カード処理端末３と、ＩＣカード４と、各サービス提供者のサービス提供サーバ５と、を備える。

【００２４】カード発行センタ１は、利用者に対するＩＣカード３の発行等を行う。このＩＣカード３の発行では、カード発行センタ１は、各サービス提供サーバ５が配信するカード用アプリケーションに基づいて、カード用アプリケーションに関する所定のテーブル（許可テーブル）を作成し、その許可テーブルに対して管理センタ２から署名の付与を受ける。そして、署名が付与された許可テーブルと所定のカード情報（カードＩＤ等）を発行対象のＩＣカード３に記録して発行する。

【００２５】カード発行センタ１により生成される許可テーブルには、例えば図２に示すように、各サービス提供サーバ５が提供するカード用アプリケーションについて、アプリケーションＩＤ、ハッシュ値等の情報が、サービス提供サーバ５を識別するためのサービス提供者ＩＤ毎に設定される。このハッシュ値は、例えばカード用アプリケーションのプログラム等、カード用アプリケーション毎に一意の情報に基づいて生成される。

【００２６】管理センタ２は、カード発行センタ１からの要求に応じて、カード発行センタ１が生成した許可テーブルに対して署名（管理者署名）を付与する。

【００２７】カード処理端末３は、ＩＣカードリーダ／ライタ等を備え、主にＩＣカード４とサービス提供サーバ５との間のデータ送受信等を行う。例えば、カード処理端末３は、利用者から入力されたカード用アプリケーションのダウンロードの要求をカードリーダ／ライタを介してＩＣカード４に通知し、これに応じてＩＣカード４から受信したカードＩＤ等をカード用アプリケーションのダウンロード要求とともにサービス提供サーバ５に送信する。また、サービス提供サーバ５から受信したカード用アプリケーションをカードリーダ／ライタを介してＩＣカード４に送信等する。

【００２８】ＩＣカード４は、ＭＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等を有するＩＣチップを備え、このＩＣチップは、例えば図３に示すように、ＭＰＵがＲＯＭ等に記憶されるプログラムを実行することにより実現される制御部４１とメモリ４２と入出力制御部４３とを備える。

【００２９】制御部４１は、カード処理端末３からの所定の通知に応じて、メモリに記憶されるカードＩＤ等をカード処理端末３に送信する。そして、制御部４１は、ダウンロードされたカード用アプリケーションをカード処理端末３から受信すると、そのカード用アプリケーションのハッシュ値を作成する。そして、受信したカード用アプリケーションのアプリケーションＩＤと、作成したハッシュ値を、メモリ４２に記憶されている許可テーブルの設定値と照合する。

【００３０】比較したアプリケーションＩＤ及びハッシュ値が一致する場合には、制御部４１は、そのカード用アプリケーションが予めカード発行センタ１に許可されたものであるとして、メモリ４２におけるカード用アプリケーションを記憶するための記憶領域に、受信したカ

ード用アプリケーションを記憶する。

【００３１】また、比較したアプリケーションＩＤ及びハッシュ値が一致しない場合には、制御部４１は、カード発行センタ１が許可したカード用アプリケーションでないと判別し、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末３にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【００３２】メモリ４２は、許可テーブル、カード情報（カードＩＤ等）、カード用アプリケーション等を記憶する。入出力制御部４３は、カード処理端末３とのデータ通信を制御する。

【００３３】サービス提供サーバ５は、ＩＣカード４へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ５は、カード処理端末３からのカード用アプリケーションのダウンロード要求に応答して、該当するカード用アプリケーションを図示せぬ記憶部から読み出して、要求元のカード処理端末３に送信する。

【００３４】次に、この第１の実施形態に係るシステムにおいて、ＩＣカード４にカード用アプリケーションを登録する場合の処理を図４を参照して説明する。例えば、ある利用者は、カード処理端末３にＩＣカード４をセットして、サービス提供サーバ５（サービス提供者ＩＤ：ＢＢＢ）が提供するカード用アプリケーション（アプリケーションＩＤ：１２３）のダウンロード要求を入力する。これに応じて、カード処理端末３はダウンロードの要求の入力をＩＣカード４に通知して、カードＩＤ等を取得し、アプリケーションＩＤ「１２３」のカード用アプリケーションのダウンロード要求とともにサービス提供サーバ５に送信する（ステップＳ１、Ｓ２）。

【００３５】ダウンロード要求を受信したサービス提供サーバ５は、該当するアプリケーションＩＤ「１２３」のカード用アプリケーションを読み出して、カード処理端末３を介してＩＣカード４に送信する（ステップＳ３）。

【００３６】ＩＣカード４は、受信したカード用アプリケーションについてハッシュ値（例えば、「２３」）を生成する（ステップＳ４）。そして、受信したカード用アプリケーションのアプリケーションＩＤ「１２３」と、生成したハッシュ値「２３」が、メモリ４２に記憶されているサービス提供者ＩＤ「ＢＢＢ」の許可テーブルの設定値と合致するかを判別する（ステップＳ５）。

【００３７】比較したアプリケーションＩＤ及びハッシュ値が合致する場合、ＩＣカード４は受信したカード用アプリケーションを、カード発行センタ１から許可されている正当なアプリケーションであるとして、メモリ４２のカード用アプリケーション用領域に格納する（ステップＳ６）。

【００３８】また、例えば、比較したアプリケーションＩＤとハッシュ値が許可テーブルの設定値と合致しない場合には、ＩＣカード４は、受信したカード用アプリケーションを、カード発行センタ１からの許可を受けていない不当なアプリケーションであるとして、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末３にエラー信号を送信する等の所定のエラー処理を実行する（ステップＳ７）。

【００３９】このようにして、ＩＣカード４に予めカード発行センタ１が許可したカード用アプリケーションに関する許可テーブルを格納しておき、ＩＣカード４にカード用アプリケーションをダウンロードする際に、そのカード用アプリケーションの正当性を許可テーブルを参照してチェックする。これにより、ダウンロードする度にカード発行センタ１にカード用アプリケーションの正当性を問い合わせることなく、カード内でその正当性をチェックすることができるため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【００４０】また、ＩＣカード４に格納される許可テーブルには、管理センタ２による管理者としての署名が付与されているため、この許可テーブルを用いてカード用アプリケーションのチェックを行うことは、カード発行センタ１と管理センタ２の両方からの許可を確認することと実質的に同意である。よって、さらにシステムの安全性を高めることができる。また、第三者的な管理センタ２による署名を付与することで、例えばカード発行元とサービス提供者の共同による不正行為等を防止することができる。

【００４１】また、管理センタ２を除いたシステム構成としてもよい。この場合、許可テーブルに第三者に管理センタ２による署名は付与されないが、上記説明のように、ＩＣカード４内で許可テーブルに基づくチェックは行うため、安全性が高く、短時間での認証が可能なカードシステムを実現することができる。

【００４２】また、各サービス提供者が提供するカード用アプリケーションが追加される場合や新たなサービス提供者が追加される場合等に、新たな許可テーブルをカード発行センタ１がカード処理端末３を介してＩＣカード４に供給するようにしてもよい。

【００４３】また、許可テーブルに記憶するチェック用データはハッシュ値に限定されない。例えば各カード用アプリケーションに対して一意な数値、データ等を導出できる任意の関数を用いても良い。

【００４４】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いても良い。この場合、利用者は、サービス提供装置にＩＣカード４をセットして、所望のカード用アプリケーションのＩＣカード４への書込要求を入力する。この入力に応じて、サービス提供装置

は、指定されたカード用アプリケーションを記憶部から読み出して、ＩＣカード４に渡す。ＩＣカード４は、上記説明と同様にして、許可テーブルに基づくカード用アプリケーションのチェックを行い、その正当性を確認した場合にはメモリ４２の所定記憶領域に記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【００４５】（第２の実施形態）本発明の第２の実施形態に係るカードシステムのシステム構成図を図５に示す。図示されるように、このカードシステムは、カード発行センタ６と、カード処理端末７と、ＩＣカード８と、各サービス提供者のサービス提供サーバ９と、を備える。

【００４６】カード発行センタ６は、利用者に対するＩＣカード８の発行等を行う。カード発行センタ６は、発行対象の各ＩＣカード８のメモリに、カード毎に一意の暗号鍵（カード用秘密鍵）を記録する。また、カード発行センタ６は、例えば図６に示すような、各ＩＣカード８のカードＩＤと暗号鍵（カード用公開鍵）を対応付ける鍵テーブルを記憶する。また、カード発行センタ６は、各サービス提供サーバ９が提供するカード用アプリケーションについて、アプリケーションＩＤと、そのカード用アプリケーションに基づいて生成されたハッシュ値が対応付けられているテーブルを記憶する。

【００４７】カード発行センタ６は、サービス提供サーバ９から、例えばカードＩＤとサービス提供者ＩＤとアプリケーションＩＤを含む鍵要求情報を受信すると、鍵要求情報に含まれるアプリケーションＩＤに対応するハッシュ値を読み出す。そして、鍵要求情報に含まれるカードＩＤに対応する暗号鍵（カード用公開鍵）を鍵テーブルから読み出し、その暗号鍵で先に取得したハッシュ値を暗号化し、暗号化されたハッシュ値に、カード発行センタ６による署名を付与して要求元のサービス提供サーバ９に送信する。

【００４８】また、カード発行センタ６は、サービス提供サーバ９から受信した鍵要求情報に基づいて、例えば図７に示すような、サービス提供者ＩＤ、カードＩＤ、アプリケーションＩＤ、登録日時等を含む課金情報を生成して記憶する。そして、この課金情報に基づいて、ＩＣカード８にカード用アプリケーションを供給するサービス提供者に対して課金を行う。課金の方法は任意であり、例えば、１アプリケーション毎に、カードへの記録時間が所定時間経過する毎に所定金額がアプリケーション提供元に課金されるようにしてもよい。

【００４９】また、カード発行センタ６は、サービス提供サーバ９から、サービス提供者ＩＤとアプリケーションの削除に関する証明書を受信すると、課金情報を参照して、受信データに該当する課金情報を特定し、その課金情報に対して、例えばアプリケーションの削除日時等の情報を設定する。なお、この証明書は、ＩＣカード８からカード用アプリケーションが削除された場合にＩＣカード８によりサービス提供サーバ９に対して発行される情報であり、例えば、削除されたアプリケーションＩＤとカードＩＤ等を含む。この証明書は、例えばＩＣカード８の秘密鍵で署名がなされていてもよい。この場合、カード発行センタ６は、ＩＣカード８の公開鍵を用いて署名を確認することにより、証明書の正当性を確認する。

【００５０】カード処理端末７は、ＩＣカードリーダ／ライタ等を備え、主にＩＣカード８とサービス提供サーバ９との間のデータ送受信等を行う。例えば、カード処理端末７は、利用者から入力されたカード用アプリケーションのダウンロード又は削除の要求等をカードリーダ／ライタを介してＩＣカード８に通知し、これに応じてＩＣカード８から受信したカードＩＤをカード用アプリケーションのダウンロード要求又は削除要求通知等とともにサービス提供サーバ９に送信する。また、カード処理端末７は、サービス提供サーバ９から受信したアクセス要求、暗号化されたハッシュ値、カード用アプリケーション等をカードリーダ／ライタを介してＩＣカード４に送信する。

【００５１】ＩＣカード８は、ＭＰＵ、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等を有するＩＣチップを備え、このＩＣチップは、例えば図８に示すように、ＭＰＵがＲＯＭ等に記憶されるプログラムを実行することにより実現される制御部８１とメモリ８２と入出力制御部８３とを備える。

【００５２】制御部８１は、カード処理端末７からの、ダウンロードの要求、カード用アプリケーションの削除の要求等が入力されたことの通知に応じて、メモリに記憶されるカードＩＤ等をカード処理端末７に送信する。

【００５３】また、制御部８１は、サービス提供サーバ９からの、ＩＣカード８へのアクセス要求（書込要求）と暗号化されたハッシュ値とカード用アプリケーション等をカード処理端末７を介して受信すると、暗号化されたハッシュ値に付与されている署名の検証を行う。そして、署名が正しければ、メモリ８２に記憶されている暗号鍵（カード用秘密鍵）を用いて、暗号化されたハッシュ値を復号化する。次に、復号化したハッシュ値を、受信したカード用アプリケーションに基づいて作成したハッシュ値と照合する。そして、比較したハッシュ値が一致する場合には、制御部８１は、メモリ８２におけるカード用アプリケーションを記憶するための記憶領域に、受信したカード用アプリケーションを記憶する。また、比較したハッシュ値が一致しない場合には、制御部８１は、カード用アプリケーションを所定の記憶領域に記憶することなく、カード処理端末７にエラー信号を送信して、エラー表示させる等の所定のエラー処理を行う。

【００５４】また、制御部８１は、サービス提供サーバ９からの、カード用アプリケーションの削除要求等をカ

ード処理端末７を介して受信すると、指定されたカード用アプリケーションをメモリ８２から削除する。そして、削除したカード用アプリケーションのアプリケーションＩＤ、そのＩＣカード８のカードＩＤ等を含む証明書をカード処理端末７を介してサービス提供サーバ９に送信する。なお、この証明書にＩＣカード８の秘密鍵を用いた署名を付与してもよい。

【００５５】メモリ８２は、暗号鍵（カード用秘密鍵）、カード発行者の公開鍵、カード情報（カードＩＤ等）、カード用アプリケーション等を記憶する。入出力制御部８３は、カード処理端末７とのデータ通信を制御する。

【００５６】サービス提供サーバ９は、ＩＣカード８へのカード用アプリケーションの提供等を行うためのサーバである。サービス提供サーバ９は、カード処理端末７からの、カード用アプリケーションのダウンロード要求に応答して、例えば、ダウンロード要求とともに受信したカードＩＤと、要求されたカード用アプリケーションのアプリケーションＩＤと、サービス提供者ＩＤを含む鍵要求情報を生成して、カード発行センタ６に送信し、暗号化されたハッシュ値をカード発行センタ６から受信する。そして、サービス提供サーバ９は、ダウンロード要求に該当するカード用アプリケーションを図示せぬ記憶部から読み出し、暗号化されたハッシュ値と所定のアクセス要求（書込要求）とともにカード処理端末７を介してＩＣカード８に送信する。

【００５７】また、サービス提供サーバ９は、カード処理端末７からのカード用アプリケーションの削除要求通知に応答して、指定されたアプリケーションの削除要求をカード処理端末７を介してＩＣカード８に送信する。そして、ＩＣカード８からの証明書をカード処理端末７を介して受信し、この証明書をカード発行センタ６に送信する。

【００５８】次に、この第２の実施形態に係るシステムにおいて、ＩＣカード８にカード用アプリケーションを登録する場合の処理を図９を参照して説明する。例えば、ある利用者は、カード処理端末７にＩＣカード８（カードＩＤ：３２３２）をセットして、サービス提供サーバ９が提供するカード用アプリケーションのダウンロード要求を入力する。これに応じて、カード処理端末７はダウンロードの要求の入力をＩＣカード８に通知して、カードＩＤ「３２３２」等を取得し、カード用アプリケーションのダウンロード要求（ダウンロード対象のアプリケーションＩＤを含む）とともにサービス提供サーバ９に送信する（ステップＳ１１、Ｓ１２）。

【００５９】ダウンロード要求を受信したサービス提供サーバ９は、受信したカードＩＤ「３２３２」と、要求されたカード用アプリケーションのアプリケーションＩＤと、サービス提供者ＩＤを含む鍵要求情報を生成して、カード発行センタ６に送信する（ステップＳ１３）。

【００６０】カード発行センタ６は、鍵要求情報の受信に応答し、この受信データに含まれるアプリケーションＩＤに対応するハッシュ値を読み出す。また、カードＩＤ「３２３２」に対応する暗号鍵「１２１２」を鍵テーブルから読み出して、その暗号鍵でハッシュ値を暗号化し、暗号化されたハッシュ値にカード発行センタ６の秘密鍵を用いた署名を付与して要求元のサービス提供サーバ９に送信する（ステップＳ１４）。また、カード発行センタ６は、サービス提供サーバ９からの受信データを用いて課金情報を生成して記憶する（ステップＳ１５）。そして、課金情報に基づいてサービス提供者がカードＩＤ「３２３２」にカード用アプリケーションを提供することに対して課金を行う。

【００６１】また、サービス提供サーバ９は、カード発行センタ６から受信した暗号化されたハッシュ値と、要求されたカード用アプリケーションと、アクセス要求（書込要求）を、カード処理端末７を介してＩＣカード８に送信する（ステップＳ１６）。

【００６２】ＩＣカード８は、受信した暗号化されたハッシュ値に付与されている署名について、カード発行センタの公開鍵を用いて検証する。署名が正しければ、暗号鍵（カード用秘密鍵）を用いて暗号化されたハッシュ値を復号化する。そして、復号化されたハッシュ値が、受信したカード用アプリケーションに基づいて作成したハッシュ値と合致するかを判別する（ステップＳ１７）。

【００６３】比較したハッシュ値が合致する場合、ＩＣカード８は、送信元の正当性を確認したとして、受信したカード用アプリケーションを、メモリ８２のカード用アプリケーション用領域に格納する（ステップＳ１８）。

【００６４】また、比較したハッシュ値が合致しない場合又は署名が不当なものである場合等には、ＩＣカード８は、例えば、そのカード用アプリケーションをカード用アプリケーション用の記憶領域に記憶することなく消去して、カード処理端末７にエラー信号を送信する等の所定のエラー処理を実行する（ステップＳ１９）。

【００６５】次に、この第２の実施形態に係るシステムにおいて、ＩＣカード８からカード用アプリケーションを削除する場合の処理を図１０を参照して説明する。例えば利用者は、カード処理端末７にＩＣカード８（カードＩＤ：３２３２）をセットして、ＩＣカード８に記憶されているカード用アプリケーションの削除要求を入力する。これに応じて、カード処理端末７はアプリケーションの削除の要求の入力をＩＣカード８に通知して、カードＩＤ「３２３２」等を取得し、カード用アプリケーションの削除要求通知（削除対象のアプリケーションＩＤを含む）とともにサービス提供サーバ９に送信する（ステップＳ２１、Ｓ２２）。

【００６６】削除要求を受信したサービス提供サーバ９は、指定されたカード用アプリケーションを削除するためのアクセス要求（削除要求）をカード処理端末７を介してＩＣカード８に送信する（ステップＳ２３）。これに応じて、ＩＣカード８は、指定されたカード用アプリケーションをメモリ８２から削除するとともに、このカード用アプリケーションを削除したことを示す証明書を作成する（ステップＳ２４、Ｓ２５）。そして、作成した証明書をカード処理端末７を介してサービス提供サーバ９に送信する（ステップＳ２６）。

【００６７】サービス提供サーバ９は、ＩＣカード８から受信した証明書をカード発行センタ６に送信する（ステップＳ２７）。カード発行センタ６は、受信した証明書からカード用アプリケーションが削除されたことを確認し、該当する課金情報にカード用アプリケーションの削除日時等を設定する（ステップＳ２８）。

【００６８】このようにして、ＩＣカード８にカード用アプリケーションを登録する時には、カード用アプリケーションの情報をＩＣカード８に固有の鍵で暗号化したものにカード発行センタ６が署名をしたものを必要とする。これにより、そのカードにしか有効でない認証用情報がカード発行センタ６により生成されるため、不正なサービス提供サーバ９によるＩＣカード８へのカード用アプリケーションの登録を排除し、安全なカードシステムを提供することができる。また、ＩＣカード８によりカード用アプリケーションの削除についての証明書を発行させて、サービス提供サーバ９にその証明書を提出させること等により、カード発行センタ６では、各ＩＣカード８へのカード用アプリケーションに登録及び削除を確実に把握できるため、適正な課金管理を行うことができる。

【００６９】また、ＩＣカード８のカード用アプリケーションを削除する場合も、登録の場合と同様に、カード発行センタ６による認証を必要とするようにしてもよい。この場合、サービス提供サーバ９は、登録の場合と同様に、カード発行センタ６から暗号化されたハッシュ値と署名を取得して、カード用アプリケーションの削除要求とともに暗証鍵をＩＣカード８に対して送信する。

【００７０】また、サービス提供者のカード用アプリケーションを記憶部に格納し、カードリーダライタを備えるサービス提供装置を用いても良い。この場合、利用者は、サービス提供装置にＩＣカード８をセットして、所望のカード用アプリケーションのＩＣカード８への書込要求を入力する。この入力に応じて、サービス提供装置は、カードＩＤとアプリケーションＩＤをカード発行センタ６に送信して、これに対する暗号化されたハッシュ値と署名をカード発行センタ６から取得し、指定されたカード用アプリケーションとともにＩＣカード８に渡す。ＩＣカード８は、上記説明と同様にして、署名及びハッシュ値のチェックを行い、その正当性を確認した場合にはメモリ８２の所定記憶領域にカード用アプリケーションを記録し、不当であると判別した場合には受け取ったアプリケーションを消去する等のエラー処理を行う。

【００７１】また、カード発行センタ６において、ＩＣカード８の暗号鍵で暗号化するものはアプリケーションＩＤに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば、アプリケーションＩＤをＩＣカード８の暗号鍵で暗号化したものに署名を付与して、サービス提供サーバ９に供給するようにしてもよい。この場合、ＩＣカード８は、署名を検証した後、暗号化されたアプリケーションＩＤを暗号鍵で復号化し、受信したカード用アプリケーションのアプリケーションＩＤであるかを判別する。

【００７２】また、カード用アプリケーションのＩＣカード８への登録に先立ってＩＣカード８が乱数を生成し、その乱数をカード発行センタ６による署名の対象に含めるようにしてもよい。この場合、例えば図１１に示すように、サービス提供サーバ９は、ＩＣカード８に対して、乱数の生成を要求する（ステップＳ３１）。これに応じて、ＩＣカード８は、乱数を生成し、生成した乱数等をサービス提供サーバ９に送信する（ステップＳ３２）。サービス提供サーバ９は、受信した乱数等と、ダウンロード対象のカード用アプリケーションのアプリケーションＩＤ等をカード発行センタ６に送信する（ステップＳ３３）。

【００７３】これに応じて、カード発行センタ６は、受信したアプリケーションＩＤに対応するハッシュ値を読み出す。そして、読み出したハッシュ値と受信した乱数をカード発行センタ６の秘密鍵で暗号化した許可情報を生成し、要求元のサービス提供サーバ９に送信する（ステップＳ３４）また、カード発行センタ６は、サービス提供者に対する課金を行う。サービス提供サーバ９は、カード発行センタ６から受信した許可情報と、要求されたカード用アプリケーションをアクセス要求とともにＩＣカード８に送信する（ステップＳ３５）。

【００７４】ＩＣカード８は、受信した許可情報をカード発行センタ６の公開鍵で復号化して、ハッシュ値と乱数を取得する。そして、取得した乱数を、自己が生成した乱数と照合する。また、ＩＣカード８は、受信したカード用アプリケーションに基づいて作成した作成したハッシュ値を、受信したハッシュ値と照合する（ステップＳ３６）。

【００７５】そして、乱数の照合結果とハッシュ値の照合結果の双方が正常である場合には、受信したカード用アプリケーションをメモリ８２の所定領域に格納し（ステップＳ３７）、いずれかの照合結果がエラーを示す場合には、そのカード用アプリケーションを所定領域に記憶することなく消去して、カード処理端末７にエラー信号を送信する等の所定のエラー処理を行う（ステップＳ

３８）。

【００７６】このようにして、乱数を用いることにより、１回限り有効な認証用情報が作成されるため、セキュリティのレベルを高めることができる。また、この例においても、カード発行センタ６における暗号化の対象はアプリケーションＩＤに対応するハッシュ値に限定されず、そのカード用アプリケーションに一意な情報であればよい。例えば乱数とアプリケーションＩＤをカード発行センタ６に秘密鍵で暗号化したものを許可情報としてサービス提供サーバ９に供給するようにしてもよい。この場合、ＩＣカード８は、復号化して得た乱数についての照合とアプリケーションＩＤについての照合を行う。

【００７７】また、上記実施例において用いる暗号方式は秘密鍵暗号方式に限定されず、共通鍵暗号方式を用いてもよい。

【００７８】また、第１と第２の実施の形態におけるカード処理端末３、７は、携帯端末（携帯電話機）等を含む。

【００７９】なお、この発明のシステムは、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、コンピュータに上述の動作を実行させるためのプログラムを格納した媒体（フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するカード発行センタ１、６、管理センタ２、カード処理端末２、７等を構成することができる。なお、上述の機能を、ＯＳが分担又はＯＳとアプリケーションの共同により実現する場合等には、ＯＳ以外の部分のみを媒体に格納してもよい。

【００８０】なお、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００８１】

【発明の効果】以上説明したように、本発明によれば、カード発行センタによる認証を受けていない供給センタによるＩＣカードへのアプリケーションの供給を排除し、安全なアプリケーションの供給を可能とする。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るカードシステムのシステム構成図である。

【図２】許可テーブルを説明するための図である。

【図３】図１のカードシステムで使用されるＩＣカードの構成を説明するための図である。

【図４】図１のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図５】本発明の第２の実施形態に係るカードシステムのシステム構成図である。

【図６】鍵テーブルを説明するための図である。

【図７】課金情報を説明するための図である。

【図８】図５のカードシステムで使用されるＩＣカードの構成を説明するための図である。

【図９】図５のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理を説明するための図である。

【図１０】図５のカードシステムにおいてＩＣカードからカード用アプリケーションを削除する場合の処理を説明するための図である。

【図１１】図５のカードシステムにおいてＩＣカードにカード用アプリケーションを登録する場合の処理の他の例を説明するための図である。

【符号の説明】

１、６　　カード発行センタ
２　　管理センタ
３、７　　カード処理端末
４、８　　ＩＣカード
５、９　　サービス提供サーバ
４１、８１　制御部
４２、８２　メモリ
４３、８３　入出力制御部

【図２】

許可テーブル

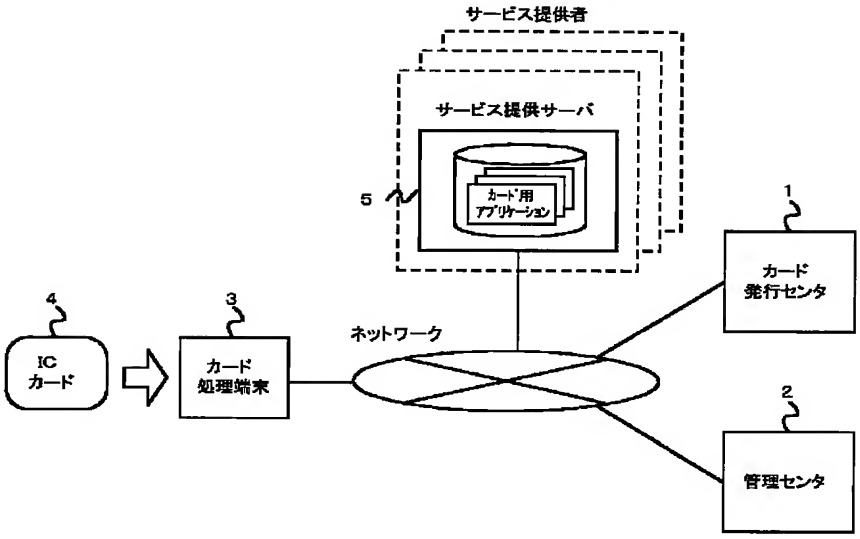
サービス提供者ID			
アプリケーションID	123	213	345
ハッシュ値	23	34	17
⋮	⋮	⋮	⋮

【図６】

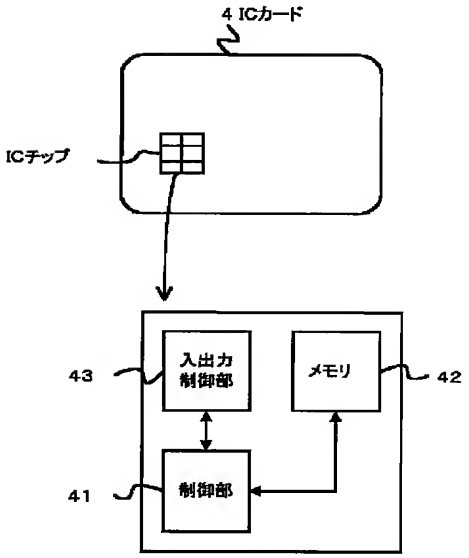
鍵テーブル

カードID	暗証鍵
9876	XXXXXX
5432	XXXXXX
⋮	⋮

【図１】



【図３】

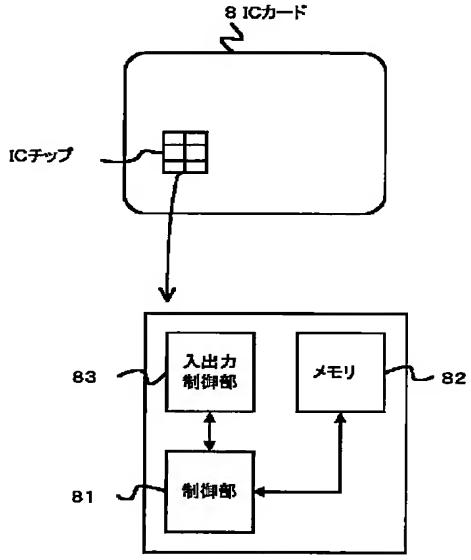


【図７】

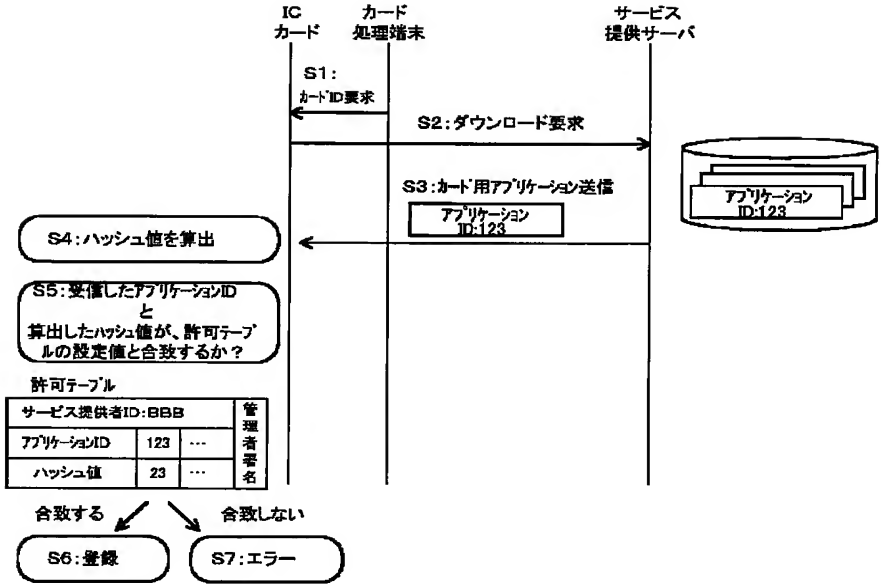
課金テーブル

サービス提供者ID	カードID	アプリケーションID	登録日時	・・・
876	1234	111	XXXX/XX/XX XX:XX	・・・
432	5678	222	XXXX/XX/XX XX:XX	・・・
⋮	⋮	⋮	⋮	⋮

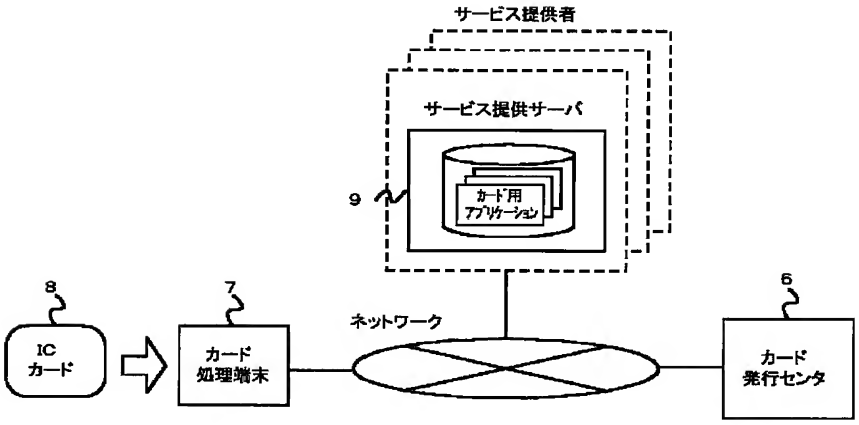
【図８】



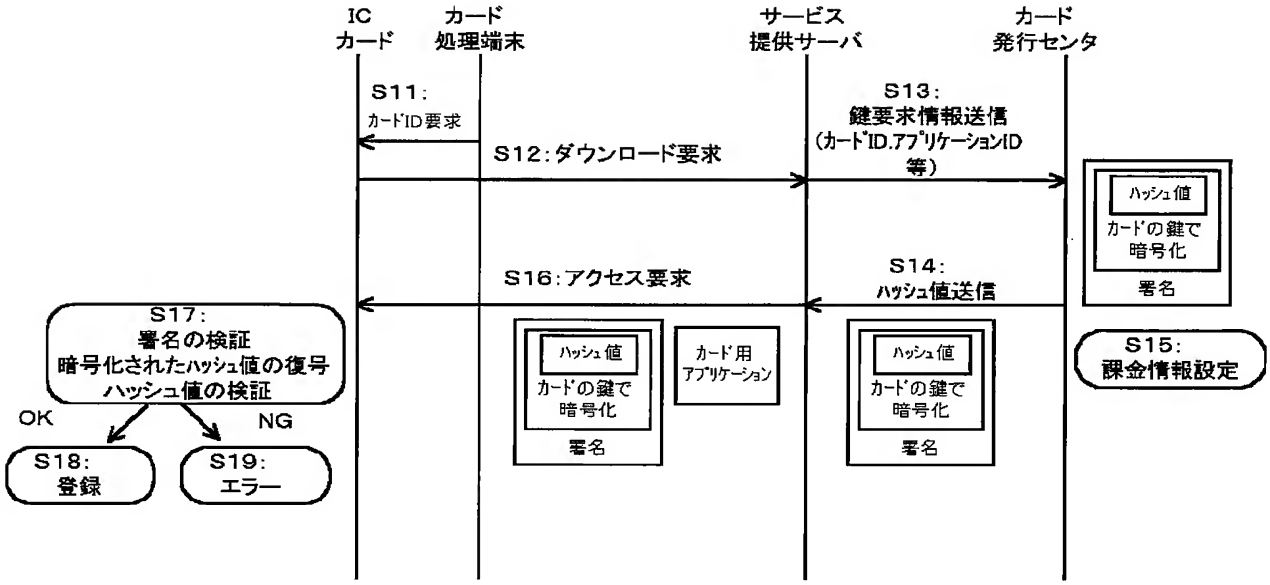
【図４】


IC
カード
カード
処理端末
サービス
提供サーバ
S1:
ｶｰﾄﾞID要求
S2:ダウンロード要求
S3:ｶｰﾄﾞ用ｱﾌﾟﾘｹｰｼｮﾝ送信
ｱﾌﾟﾘｹｰｼｮﾝ
ID:123
ｱﾌﾟﾘｹｰｼｮﾝ
ID:123
S4:ハッシュ値を算出
S5:受信したｱﾌﾟﾘｹｰｼｮﾝID
と
算出したハッシュ値が、許可ﾃｰﾌﾞ
ルの設定値と合致するか？
許可ﾃｰﾌﾞﾙ
サービス提供者ID:BBB
ｱﾌﾟﾘｹｰｼｮﾝID
123
…
ハッシュ値
23
…
管理者署名
合致する
合致しない
S6:登録
S7:エラー

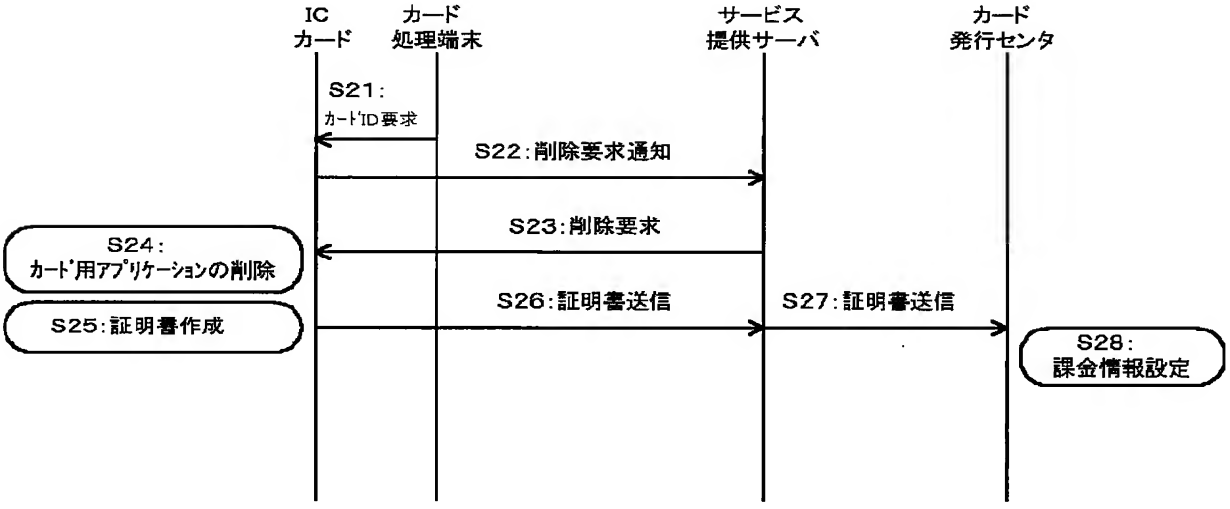
【図５】


サービス提供者
サービス提供サーバ
9
ｶｰﾄﾞ用
ｱﾌﾟﾘｹｰｼｮﾝ
8
7
6
ネットワーク
IC
カード
カード
処理端末
カード
発行センタ

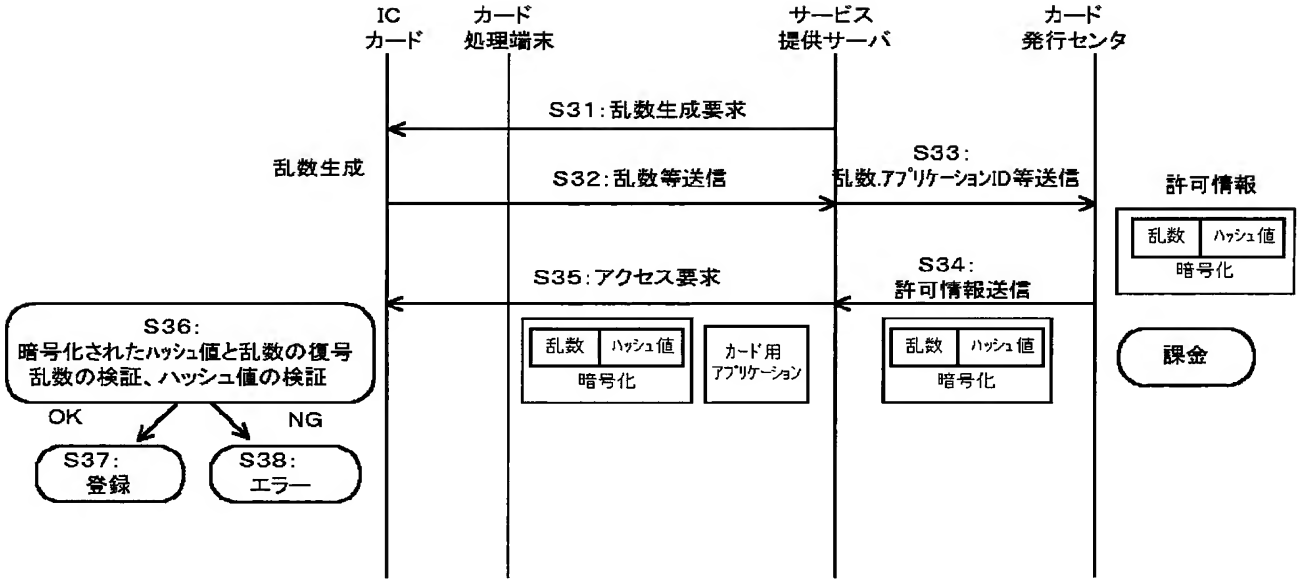
【図９】


IC
カード
カード
処理端末
サービス
提供サーバ
カード
発行センタ
S11:
カードID要求
S12:ダウンロード要求
S13:
鍵要求情報送信
(カードID,アプリケーションID
等)
ハッシュ値
カードの鍵で
暗号化
署名
S14:
ハッシュ値送信
S15:
課金情報設定
S16:アクセス要求
S17:
署名の検証
暗号化されたハッシュ値の復号
ハッシュ値の検証
OK
NG
S18:
登録
S19:
エラー
ハッシュ値
カードの鍵で
暗号化
署名
カード用
アプリケーション
ハッシュ値
カードの鍵で
暗号化
署名

【図１０】


IC
カード
カード
処理端末
サービス
提供サーバ
カード
発行センタ
S21:
カードID要求
S22:削除要求通知
S23:削除要求
S24:
カード用アプリケーションの削除
S25:証明書作成
S26:証明書送信
S27:証明書送信
S28:
課金情報設定

【図１１】



フロントページの続き

(51) Int. Cl.[7] 識別記号 F I テーマコード(参考)

Ｇ０６Ｋ 19/00 Ｇ０６Ｋ 19/00 Q

(72) 発明者 雨宮 俊一
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72) 発明者 玉井 純
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72) 発明者 冨永 洋
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内
(72) 発明者 高木 聡一郎
東京都江東区豊洲三丁目３番３号 株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考) 5B035 AA06 AA13 BB09 CA29
5B058 KA11 KA31 KA33
5B076 BB06 FB02 FB09